Saldanha Bay Municipality

Risk Management Strategy
Inclusive of, framework,
procedures and methodology

REPORT TO	PORTFOLIO / MAYCO / COUNCIL
DEPARTMENT	STRATEGIC AND ENTERPRISE RISK SERVICES
ITEM NO	
FILE NO	
DATE	MARCH 2016

REVISION TABLE

Description	Date adopted / reviewed	Resolution
Adoption of risk management strategy	26 October 2010	R22/10-10
First review	March 2015 – March 2016	

Contents

1   Introduction

Risk is part of every human effort, and an integral part of both profit and non-profit business undertakings. Organizations and leaders of these organizations are routinely exposed to risks of different degrees towards the attainment of goals and objectives.

Local municipalities as the third sphere of government provide a range of municipal services to their communities.   Further, the municipality has recognized that innovation and accountability are essential in the pursuit of its mandate. To ensure that the stated objectives are achieved in the complex and dynamic environment within which the municipality operates; and without compromising our stakeholders trust and quality of our service; an effective approach to management of risks that are faced on an ongoing basis is needed.

While the ultimate responsibility for risk management rests with Council and the Accounting Officer, it is the responsibility of all management and officials, to ensure that risk management is integrated in Saldanha Bay's decision making processes and operations. Management must therefore embrace risk and in so doing, actively consider it in strategy and objective setting as well as in undertaking and performing their day to day duties and responsibilities.

1.1   Legislative Framework and best practice

One of the prescripts of the Municipal Finance Management Act (MFMA) is that municipalities should design and implement risk management practices. This is to enable the political and administrative leadership to proactively plan their risk mitigation strategies for the achievement of strategic objectives as outlined in the municipalities' Integrated Development Plans (IDP), and as mandated in

terms of this Act (MFMA), the Municipal Systems Act, regulations, and other government prescripts.

It is required in terms of section 62 of the Municipal Finance Management Act (MFMA), no. 56 of 2003, that the Accounting Officer should take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent systems of financial and **risk management** and internal control as well as the effective, efficient and economical use of the resources of the municipality.

Furthermore, Section 78(1)(a) of the MFMA requires that: "Senior managers and other officials of municipalities;

(1)…must take all reasonable steps within their area of responsibility to ensure

(a) That the system of financial management and internal control established for the municipality is carried out diligently"

1.2   Purpose of Enterprise Risk Management

"*Enterprise risk management provides a framework for management to effectively deal with uncertainty and associated risk and opportunity, and thereby enhance the capacity to build value.*"

The purpose of the strategy therefore, is to create robust structures, systems and processes that will minimize risk, enhance opportunities while achieving the objectives of Saldanha Bay Municipality thereby enhancing stakeholder value. It also serves as a tool to improve awareness and responsibilities for the management of risks at all levels of the Municipality.

Furthermore, the strategy aims to create a strong risk management culture while enabling Saldanha Bay Municipality to comply with applicable legislation.

1.3   Scope and Applicability

The risk management strategy applies across the municipality, political and administrative levels, all levels of employment and all activities.   Risk management should therefore be considered at strategic levels (design); tactical levels as well as at operational levels, to ensure that strategies are in place to manage the risks within acceptable levels; thereby ensuring the achievement of strategic objectives.

Risk management shall therefore be considered in the design and development of Saldanha Bay Municipality's strategic goals and objectives; strategy implementation and operational plans; and compliance with legislation.

1.4   Definition of Risk and Terms

1.4.1   Definition of risk

"*The threat that an event or action will adversely affect an organization's ability to achieve its business objectives and to execute its strategies successfully.*"

The main components of risk are:

• The probability of occurrence or non-occurrence

• The root cause of the uncertainty

- The qualitative and/or quantitative impact of the risk.

The risk definition therefore takes into account:

- the <u>downside to risk</u>, which is the possibility of loss or deviations from expected outcomes; and

- the <u>upside to risk</u>, which is the possibility of business opportunities that can be exploited towards the fulfillment of strategic objectives.

The Municipality may be exposed to different categories of risks (**refer Annexure A**) which may be internal or external to the organization. External risks are those where the municipality has little or no control over their occurrence but may have an impact on the achievement of objectives.

1.4.2   Definitions of Terms Referred to in the Risk Management Strategy

"**Councillor**" means a Councillor of the municipal council of the Saldanha Bay Municipality.

"**Executive Mayoral Committee**" mean Council members who are appointed to the Executive Mayoral Committee inclusive of the Mayor, Deputy Mayor, Speaker and the respective Portfolio Councillors.

"**Audit Committee**" mean members of the Committee established in terms of section 166 of the MFMA.

"**Accounting Officer**" means the Municipal Manager.

"**Committee**" means the Risk and Fraud Committee of the Municipality.

"**COSO**" means the Enterprise Risk Management – Integrated Framework (2004), issued by the Committee of Sponsoring Organisations

"**Executive Management Team**" inclusive of Municipal Manager appointed in terms of section 55 of the Municipal Systems Act and Directors appointed in terms of section 56 of the Municipal Systems Act.

"**Business Process**" the business process is a series of activities designed by management, and carried out by officials employed in a department.

"**Internal Control**" is a "… process, effected by an entity …, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives …" in the following categories:

- Reliability and integrity of information;

- The effectiveness and efficiency of operations;

- Safeguarding of assets;

- Compliance with applicable laws and regulations, policies, plans, procedures.

"**Inherent Risk**" is the risk attached to a business process **before taking into account** any existing internal controls. It is a risk that exists because the process exists.

"**Impact**" is the potential magnitude of the impact on the municipality's operations should the risk/threat actually occur. This is assessed on the basis that management have no specific/focused controls in place to address the risk/threat.

"**Internal Control Adequacy**" refers to the design of the processes, systems, and resource requirements by management and/or the Council to ensure the achievement of objectives. The design of an internal control system is largely informed by its capability to mitigate the impact of risks or the capability to exploit an opportunity.

"**Internal Control Effectiveness**" is an assessment of the effectiveness of existing controls at managing the potential impact of inherent risk. It is assessed on the bases of the existence of controls and a judgment as to their effectiveness.

"**Likelihood**" is the possibility or probability of occurrence or non-occurrence (the identified risk may or may not occur).

"**Residual Risk**" is the risk exposure that the municipality/unit/department will remain exposed to after the design and/or implementation of risk mitigating responses.

"**Risk Appetite**" is the degree of risk, on a broad based level, that the municipality is willing to accept in pursuit of its goals; and is informed by the risk environment within which the municipality operates.

"**Risk Assessment**" is a continuous process of identifying, analyzing, measuring and prioritizing risks / threats that may or may not occur.

"**Enterprise Risk Management**" is a continuous process that can be defined as the identification and assessment of actual and potential risks that the municipality/ department may be exposed to, ensuring that appropriate structures, policies and procedures are in place to manage these risks, and the design and introduction of responses or controls to pro-actively manage or mitigate the risk probability and impact. This assessment requires management decisions to accept, avoid, transfer or control the risks, or a combination of

these options. Risk Management also includes the identification of areas of opportunity, and therefore the risks that should be taken in pursuance of these opportunities, with appropriate strategies to mitigate against avoidable losses.

"**Risk Mitigating**" refers to risk reduction to a certain level. This takes into account those risks that cannot be eliminated entirely, but with the implementation of some control measures can be reduced to an acceptable level.

"**Risk Threshold levels**" these are the levels of risks applicable during a given financial period. It is the level of risk exposure that, in the opinion of the Risk Committee, is of a significant nature; the amount and the management thereof should be communicated to the Executive Mayoral Committee and Council.

"**Risk Tolerance**" the amount of risk the Municipality is capable of bearing as opposed to the amount of risk it is willing to bear.

"**Risk Universe**" includes all the legislation (acts and regulations); the strategic intentions as outlined in the IDP, SDBIP and the municipality's Organizational Performance Scorecards, business plans; operations and activities of the municipality.

1.5   Enterprise Risk Management Process

Enterprise risk management is a continuous, proactive and systematic process to understand, manage, monitor and communicate risk from an organization-wide perspective. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives; and is affected by people at every level of an organization. It is a multidirectional, interactive process in which almost any component can and does influence another.

The risk management decisions that can be taken by management include strategies such as <u>risk avoidance</u>; <u>risk transferring</u>, <u>diversification (outsourcing)</u>; <u>accepting or tolerating the risk</u>; <u>risk control or treatment</u> to acceptable levels.

The risk management process eight elements of the COSO framework (refer to Integration of the ERM process in achievement of objectives under 5. Enterprise Risk Management Process) can be simplified into FOUR main steps:

The Confirmation / Understanding of organizational Goals and Objectives:

- Establishing and obtaining understanding of the goals and objectives of Saldanha Bay Municipality; its mission, vision and core-values.

- Establishing and obtaining the understanding of goals, objectives and strategies, of the various departments/business units. This will include:

  o Establishing how these are aligned to the overall organizational goals and objectives.

  o Identifying the key processes, and sub-processes or activities.

Conducting Inherent Risk Assessments [Strategic and/or Operational]

- Identifying risks associated with the strategic objectives, priorities, or key processes and activities.

- Assessing the likelihood that the event may occur and the impact should it occur?

- Assess significant trends and changes in Key Risk Indicators.

- Measuring the associated inherent risk, which will include assessing the value of the organization's assets that are at risk?

Risk Response /Control/ Mitigation (Managing the Risks to acceptable threshold levels)

- Establishing the risk management strategies in place and assessing their adequacy.

- Deciding and designing risk management strategies where "gaps" have been identified.

- Assigning responsibilities and accountability, timeframes (as appropriate), for the design and/or implementation.

- Financing the risk management strategies.

- Implementing the risk management strategies.

- Assessing the effectiveness of the risk management strategies.

- Measuring the residual risk exposure.

Risk Monitoring and Communication

- Continuously monitoring the effectiveness of the risk management strategies.

- Communicate and report on the risk management profile and strategies.

- Conducting Assurance reviews and reporting.

The Enterprise Risk Management Process is a continuous cyclical process. The integration of the process in the achievement of the municipality's objectives is depicted in (refer to Integration of the ERM process in achievement of objectives under 5. Enterprise Risk Management Process) of this framework.

2   Risk Management Principles

The Risk Management principles shall be observed at all times; and should be read together with the roles and responsibilities for risk management as outlined under 4. Governance Structure, Roles and Responsibilities; as well as with the risk management procedures outlined under 7. Enterprise Risk Management Procedures:

- The organization-wide commitment to effective risk management will start at the top of the municipality (Council and its Committees, Accounting Officer and Directors).

- Risk management shall be embedded into the culture of the municipality and operations such as strategic planning, financial planning, policy making and review, and performance management. Accordingly, the assessment of risks shall commence at strategy design, development and planning processes of the municipality.

- Managing risk shall be everyone's responsibility, paying equal attention to quantitative and qualitative risks.

- The importance of discipline, prudence and respect for limits, in all risk-taking activities may not be undermined. Accordingly, delegations of authority shall be set and complied with.

- Risks should be taken on the basis of rigorous analysis that reflects a systematic approach to the risk management process.

- Risks will be diversified and transferred to avoid undue concentration of /or exposure to risks.

- Risks will be monitored closely because constant changes in the operating environment affect their value and importance.

- Risks will be controlled carefully to ensure that the relationship between capital, risk, and reward of service delivery is managed within the boundaries of the management strategy.

- Risks should be taken in moderation relative to available capital resources and in response to service delivery opportunities.

3   BENEFITS OF RISK MANAGEMENT

Description	Benefit
Organizational Alignment	The risk management process is designed to complement effective strategic and operational planning. It will assist in ensuring that management and staff understand, and are committed to the Strategic Focus Areas which have been defined in the IDP and the SDBIP. This will include an understanding of the key performance indicators (KPI's) against which our success is measured.
Service Delivery	The overall benefit of risk management is effective and efficient service delivery. Realising "quick wins / low hanging fruit" and prioritize deployment of capital.
Manage Risk	The formal identification and evaluation of risks will improve management and staff's understanding of the risks which need to be managed, therefore the risk appetite and profile of the municipality. Furthermore, it will enable the analyses and understanding of the causes of risks to ensure effective internal controls to manage these causes.
Achieve Objectives	By proactively identifying risks, the Municipality will have a better understanding of risks and be more anticipatory and therefore able to achieve its objectives with greater certainty.
Seize Opportunities	By understanding its risk profiles, the risk management process will enable management to seize and execute new opportunities successfully.
Cost Effective Internal Control	The risk management process will ensure that the system of internal control is cost effective. Areas of over control should be identified and removed.

4 GOVERNANCE STRUCTURE, ROLES AND RESPONSIBILITIES

4.1 ERM Governance Structure

The responsibility for the risk management function shall be in accordance with the provisions of the Municipal Finance Management Act; be aligned to the King III Code on corporate governance, as well as the COSO Enterprise Risk Management framework.

While one of the municipality's risk management principles is to ensure that everyone is responsible for managing risks, in embedding the enterprise risk management process, it is important to ensure that there is delineation of roles and responsibilities. Accordingly, the municipality has developed a governance structure:

Role	Responsible Functionaries
Oversight	Council and Executive Mayoral Committee
Monitoring	Executive Mayoral Committee
Stewardship	Risk and Fraud Committee
Implementation	All Councillors and Officials of the Municipality
Assurance	Internal Audit Activity and Provincial Treasury (Corporate Governance)

4.2 Roles and Responsibilities of Council / Executive Mayoral Committee

Council and Executive Mayoral Committee is required to:

- Approve the Risk Management Policy and Strategy upon the recommendations of the municipality's Risk and Fraud Committee.

- Review and approve risk threshold levels, the top strategic risk register, and risk mitigation strategies and plans. Furthermore, Executive Mayoral Committee should monitor through the Risk and Fraud Committee the quarterly reports on performance against set strategic focus areas pertaining to risks.

- Monitor the risk mitigation strategies for those areas and activities with extreme to high inherent and residual risk exposures (the top risks).

Council and Executive Mayoral Committee should when reviewing its reports:

- Assess the effectiveness of the related system of internal control in managing the significant failings or weaknesses in internal control that have been reported.

- Consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

- Review the Risk and Fraud Committee minutes of meetings and/or any reports that are submitted.

Council shall through the approval of the Risk and Fraud Committee terms of reference, delegate the responsibilities to review the risk management

processes and the high risk exposures of the municipality to the Committee, in order to discharge its (Council's) duties with regard to risk management.

4.3　Roles and Responsibilities of the Risk and Fraud Committee

The Committee's responsibilities relating to risk management are as outlined in the terms of reference of the Committee approved by Council.

The Committee's responsibilities include:

- Reviewing the policies and overall process for identifying and assessing business risks and managing their impact.

- Recommending the Municipality's key risk management policy and/or strategy for ratification; and giving appropriate advice on risk threshold levels.

- Reviewing and discussing the risk management and compliance initiatives planned for the year and the results thereof.

- Examining the manner in which management ensures and monitors the adequacy of the nature, intent and effectiveness of the risk and control infrastructure of the Saldanha Bay Municipality.

- Review the identification of risks processes, programs and measures in place to mitigate the inherent risks identified for strategic, financial, compliance and operational areas as well as the implementation thereof.

- Review the identification of fraud and corruption risks, anti-fraud programs and measures in place to mitigate the inherent risks identified as well as the implementation thereof.

- Reviewing regular assurance reports from management, internal audit, auditor-general and other assurance providers on the operational adequacy and effectiveness of matters related to risk and control and the conclusions of any testing carried out on them; and

- Reviewing the timeliness of, and reports on, the effectiveness of corrective action taken by management.

4.4 Roles and Responsibilities of Senior Management

Municipal Manager is responsible in consultation with the Municipal Council for determining the strategic direction of the municipality; and ensuring that effective and efficient risk management processes are implemented throughout the municipality to manage risks that can significantly impact on the achievement of service delivery objectives.

Municipal Manager's responsibilities include the following:

- Establishing an integrated risk management system throughout the municipality.

- Delegating appropriate levels of authority and decision making to enable the effective and efficient implementation of the risk management system and strategies.

- Monitoring the performance of the risk management mitigation and management of the strategic risk areas specific to the directorates, and those that are cross-cutting. This entails the inclusion of the management of risks as a Key Performance Indicator (KPI) for the Executive Management Team, Senior Management Team and Operational Management Team.

- Ensuring that reports are submitted to the Committee and Council; on the municipality's risk environment and profile.

- Receiving the annual report on the municipality's Risk Management activity.

The Municipal Manager should oversee the achievement of strategic focus areas and municipal priorities as defined in the strategic and operational plans for the design and implementation strategies to mitigate the risks at strategic, tactical and operational levels.

The responsibilities of the Executive Management Team include the following:

- Formal responsibility for overseeing the enterprise risk management process, in their specific directorates and across the municipality.

- Review and suggest amendments of the risk management policy, strategy, appetite, tolerance and processes annually and set the risk threshold levels.

- Reviewing and oversee the implementation of the risk management policy and strategy.

- Consider what the significant risks are and assess how it have been identified, evaluated and managed.

- Consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses.

- Design the Key Performance Indicators (KPI's) for the implementation of risk management processes and action plans for each Manager reporting directly.

- Receive quarterly reports to review, scrutinize, and challenge current and proposed risk management procedures and processes, including progress

against planned actions detailing risks to municipal objectives and priorities. Monitor significant trends and changes in Key Risk Indicators.

- Monitor progress on the implementation of risk mitigation responses to bring strategic, tactical and operational level risks to acceptable levels; and report to the Committee on the adequacy and effectiveness thereof.

4.5 Roles and Responsibilities of Executive Management Team, Senior Management Team, Operational Management Team and Supervisors

The responsibility for implementing risk management processes is essentially that of all (Councillors and Officials) the Management representatives within Saldanha Bay Municipality.

Management representatives are responsible for ensuring that the risk management policy and strategy is implemented at all levels and therefore embedding risk management in the organizational culture.   This level of management should:

- Conduct continuous risk assessment.

- Identify effective, economical and efficient risk management strategies – avoid, transfer, accept, control.

- Ensuring that risk management strategies adopted are implemented, adequate and effective.

- Determining and monitoring the respective Unit's Key Risk Indicators (KRI's) on an ongoing basis.

- Monitoring the performance of direct reportees in the implementation of action plans.

Directors should manage the performance of their direct reportees in the implementation of actions plans to mitigate identified risks. Accordingly, the Directors shall develop the Key Performance Indicator (KPI) for the management and/or senior team; and ensure its inclusion in the individual performance plan.

4.6 Roles and Responsibilities of Management and Officials

The role and responsibilities of operational management include:
- Maintaining awareness of risks, their impact and associated costs.
- Implementing risk management processes
- Controlling risks in their every day-to-day work.
- Monitoring progress in managing job-related risks, and reporting to the Supervisor, Operational Manager, Senior Manager, and then Director.

Successful implementation of the risk management process highly depends on the availability and reliability of information. Therefore, management of the various business units that are custodians of information will have a duty to ensure the availability of such information.

4.7 Roles and Responsibilities of the Enterprise Risk Services

The Risk Management Unit – Consulting services

The risk management function must champion the establishment and maintenance of the municipality's Enterprise Risk Management process and systems.

Must develop the enterprise risk management policy and strategy; and the risk assessment methodology; for recommendation of adoption by the Committee and Council.

The unit must, in facilitating the implementation of the ERM process, be responsible for the following:

- Researching and benchmarking the municipality's ERM process against good practice
- Creating management and municipal-wide awareness of the ERM process and associated benefits
- Support the integration and embedding of ERM in the municipality's strategic and daily operations

The following consulting roles:

- Facilitating strategic and operational /departmental risk assessments (identification, analysis, evaluation and measurement of inherent and residual risks).

- Consulting advice to management in responding to risks.

- Co-ordinating Enterprise-Wide Risk Management activities.

- Consolidating the reporting on risks.

- Liaising with the Auditor General as and when necessary.

4.8   Roles and Responsibilities of the Internal Audit Activity

Internal Audit Assurance activities

The management of risks is a key responsibility of management, as outlined above. However, in accordance with business practice as well as in terms of the Institute of Internal Audit Standards the internal audit function acting in a <u>consulting</u> role shall assist the organization in identifying, evaluating, and implementing risk management methodologies and controls to address those risks.

Developing assessments and reports on the municipality's risk management processes is normally a high audit priority.

The role of internal audit function must be in line with its mandate as outlined in the approved Internal Audit Charter. The function shall include the following:

- Reviewing and providing assurance that the risks of the organization are being systematically identified, evaluated and appropriately managed.

- Utilizing the results of strategic and operational risk assessments to identify areas of high risk and therefore direct its efforts to monitor and evaluate the adequacy and effectiveness of the risk mitigation responses designed by management.

- Reporting on the effectiveness of the enterprise risk management process and procedures. Based on the results of internal audit projects undertaken, Internal Audit shall report on the effectiveness of the system of internal controls.

The Manager: Internal Audit shall be in attendance at all meetings of the Risk Committee strategic risk management processes are considered and approved.

The Manager: Internal Audit shall report to the Audit Committee on the municipality's progress in implementing the enterprise risk management system and processes; and the municipality's risk profile.

5   THE ENTERPRISE RISK MANAGEMENT PROCESS

Risk management has progressed from the traditional approach of managing risk in isolation whereby responsibility for different types of risks vest primarily in functional service organizations, towards a municipal-wide, integrated approach of managing risk and reward (opportunities) across Saldanha Bay Municipality and at every level. The integrated risk management approach recognizes the inter-related and interdependent nature of risk, both at strategic and at operational levels.

The Saldanha Bay Municipality's framework is aligned to the COSO Enterprise Risk Management – Integrated framework. The municipality's framework encompasses the:

The Enterprise **Risk Management Infrastructure** which comprises the following:

- The Risk Management Governance Structure

- Risk management policies

- Common risk language / glossary of terms

- Risk assessment tools and methodology

- Information Technology

- Risk threshold and tolerance levels

The **Enterprise Risk Management (ERM) Process**, which focuses on the organizational goals, objectives and strategy, is cyclical in nature. The ERM process, as illustrated below, includes:

- Identification or establishment of organizational objectives using the four categories, viz: Strategic, Operational, Compliance and Service Delivery

- Risk Identification, Assessment (analysis, measurement) and Prioritization:

- Identification and design of risk mitigation strategies and responses, as well as capabilities (risk avoidance/termination, risk tolerance, risk transfer, risk treatment /control)

- Implementation of risk mitigation strategies and action plans

- Measuring the risk exposure, monitor and communicate results

- Integrate results with decision making processes
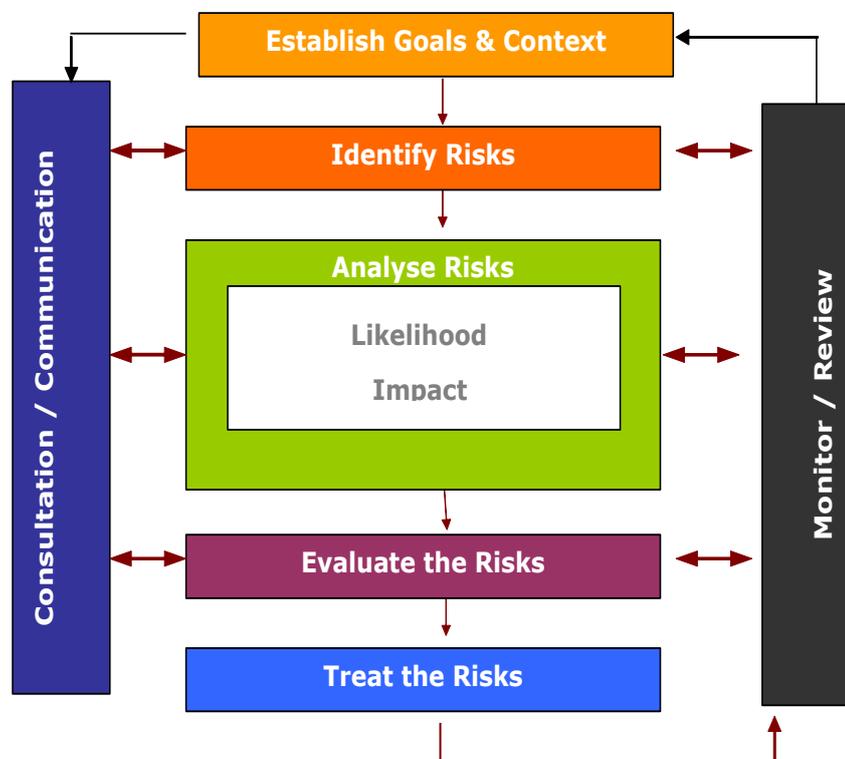
An Enabling Environment

The establishment and maintenance of an **enabling environment** includes information sharing processes; awareness and training on risk management; communication; change management; and continuous improvement.

Availability and furnishing of information for risk management purposes is the responsibility of management.

The risk management function should ensure the availability and reliability of the risk management software and therefore the risk database and profiles.

Risk Categories / framework

The Municipality may be exposed to different categories of risks (refer **Annexure A**) which may be internal or external to the organization. External risks are those where the municipality has little or no control over their occurrence but may have an impact on the achievement of objectives.

Internal risks have been classified into four main categories namely: Strategic, Financial, Compliance/Regulatory; and Service Delivery risks.

- **Strategic:** which prevent the municipality from reaching its strategic goals based on poor strategic planning, corporate or operating structure or business models.

- **Financial:** include funding resources, cash flow management, counterpart risk, investment risks and credit risks.

- **Compliance / Regulatory:** associated with the failure to comply with various regulatory requirements governing municipalities in South Africa.

- **Service Delivery:** loss due to deficiencies or failures in operational processes, people, information systems, and management failures

External risks may include macro-economic conditions; globalization; regulatory effects; public image; risks associated with external stakeholders.

The service delivery risks can be further categorized into: process / business operations; human capital management; information and communications technology; communication and management information; fraud and corruption.

Integration of the ERM process in the achievement of objectives

The COSO ERM Integrated framework has been adopted to ensure the integration of the enterprise risk management process in the achievement of objectives.
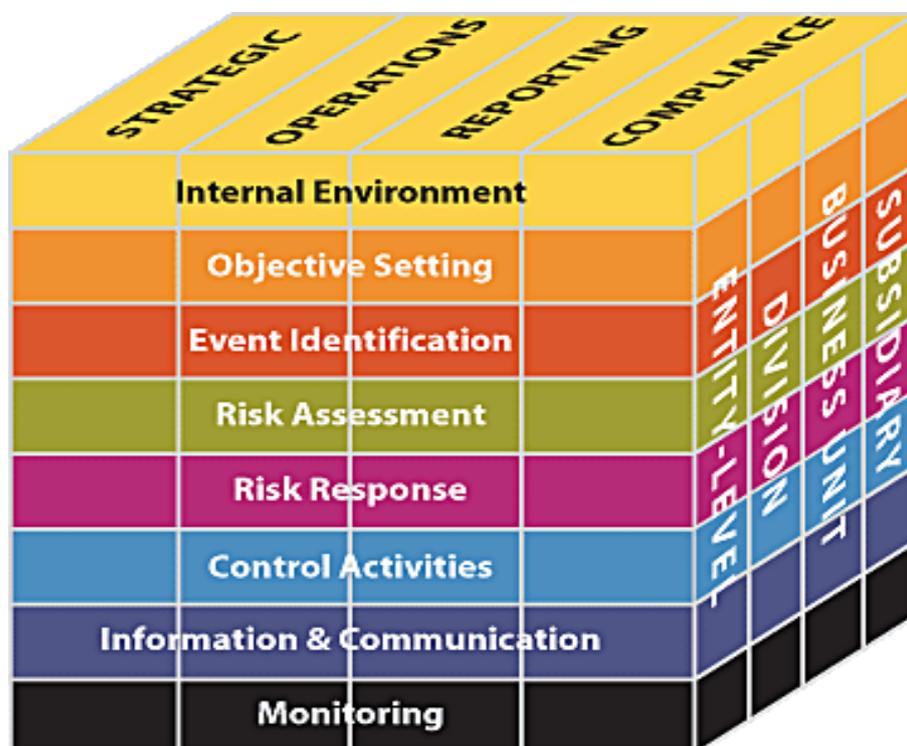
The COSO framework as depicted above, is designed to depict the integration of the eight elements of the ERM process (defined below) with the four main

categories of organizational objectives; in each of the business units and at all levels of employment.

The eight elements of the Enterprise Risk Management Process (grouped into four main categories):

1.1 *Internal Environment* – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

1.2 *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align the entity's mission and are consistent with its risk appetite.

2.1 *Event Identification* – Internal and external events affecting the achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

2.2 *Risk Assessment* – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

3.1 *Risk Response* - Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

3.2 *Control Activities* – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

4.1 *Information and Communication -*   Relevant information is identified, captured and communicated in a form and timeline that enable people to carry out their responsibilities.   Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

4.2 *Monitoring -* The entirety of enterprise risk management is monitored and modifications made necessary.   Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Risk Mitigation Strategies

The Managers of Departments will have the authority to decide on the strategies adopted in their business units and/or in their areas of responsibility. This authority shall be subject to the Delegation of Authority Policy and Framework.

The main purpose of treating or mitigating the identified risks is to:

- Reduce the likelihood of the occurrence/non-occurrence of the event;

- Reduce the possible impact should the risk occur.

The main strategies or a combination thereof can be used to mitigate identified risks; while the choice thereof should always be informed by an analysis of the cost vs. benefit:

- Risk Avoidance   (Terminate)

- Risk Transfer   (Transfer)

- Accepting the risk   (Tolerate)

- Controlling the risk   (Treatment)

The risk mitigation strategies could include, but not be limited to the following:

- Delineation of Responsibilities and Delegation of Authority;

- An internal control framework and cost-effective internal controls;

- Understanding of the "upside to risks" – opportunities;

- Business Continuity vs. "Crisis" Management;

- Project Risk Assessments [Cost vs. Benefit Analysis, Feasibility Studies, Alignment to Strategic Objectives];

- Understanding of Conflict Priorities and Critical Path Analysis;

- Fraud Risk Management [Fraud Assessments and Fraud Prevention Plan].

The following strategies are self-explanatory but can be understood to mean the following:

Risk strategy	Description / Definition
Risk Avoidance	Avoiding a risk involves side-stepping it altogether by not investing any of the municipality's resources. It may involve the redesign of the business process to change the inherent risk pattern.
Risk Transfer / Insure	Risk transfer involves transferring the threat elsewhere and therefore the impact thereof. If outsourcing is adopted as a strategy, management will be responsible for the management of associated risks
	Risk Insure is adopted to ensure protection against financial loss arising from the impact of the risk occurring.
Risk Acceptance	This strategy involves the decision to accept the threat associated with that activity or function. It is most appropriate where both the probability of occurrence as well as the potential impact should it occur are low.
Risk Control	The decision to reduce the risk by controlling it, involves the implementation of controls that Management shall design to reduce either the probability of occurrence and/or the impact should it materialize. The municipality aligns itself to the COSO Internal control framework.
	This could also include Risk Diversification, which is spreading the total risk over a number of operations, such as sourcing similar services or products from different service

	providers.
	One of the key internal control systems includes Business Continuity Management Planning/ disaster recovery.

6   ENTERPRISE RISK ASSESSMENT & METHODOLOGY

The Enterprise-Wide Risk Assessment process requires the assessment of strategic risks and operational risks which are risks at the business unit process level.

Strategic Risk Assessments:

It is good practice to commence risk assessments with a strategic risk assessment as this requires the assessment of risks that could impact on the achievement of the Municipality's goals and objectives. These could be internal and external risks and usually will be assessed at the level of Municipal Manager, the Directors and the Managers.

Process Risk Assessments:

The process risk assessments normally follow the strategic risk assessments, wherein every effort is made to ensure alignment.   These assessments are at business unit level and will focus on the key strategic focus areas and/or key processes of each business unit.   Accordingly, these assessments are at directorate level with the Municipal Manager, Directors, Managers, Supervisor and/or Senior Officials.

Inherent risk assessments:

Inherent risk assessment is an analysis of the cause of the **uncertainty**, the **likelihood** of this uncertainty occurring, and the **impact** attached to a process or operation, **before** taking into account any existing controls.

- The main steps in the Inherent Risk Assessment are: Risk Identification; Risk Analysis; Risk Measurement and Risk Prioritization.

- The municipality has adopted a five by five matrix for the assessment of inherent risk; i.e. for the likelihood of occurrence or non-occurrence and the impact or potential loss. The risk assessment tables are attached as **Annexure B**

- The inherent risk is calculated as follows:

= **Potential Loss** / **Impact** (Qualitative or Rand Value) X **Likelihood of Occurrence**

- The measured risk result (Impact and Likelihood) provides an indication of the type of risk management strategy that should be adopted (which risks should be managed) to ensure focus of effort on areas of greatest risk.

Residual risk assessments:

Residual risk is the uncontrollable risk, which is the risk that the municipality will still be exposed to having designed and implemented risk management strategies. It is the risk appetite of the organization after the adequacy and effectiveness of the controls to mitigate risk have been evaluated.

The measurement of the residual risk exposure, therefore, follows the identification and evaluation of the risk management strategies. It consists of the following three main components:

- Assessing the **level** of **inherent risk** associated with each strategy, process or functionality

- Assessing the **adequacy and effectiveness** of internal controls to mitigate the inherent risks. This necessitates a review of the design of the control activities for adequacy to mitigate the identified risk; as well as the implementation of the control activities for effectiveness to mitigate the identified risks

- **Assessing** the residual uncontrolled **risk**

- The residual risk is calculated as follows

Risk Exposure = Inherent Risk X (1 – Control Adequacy / Effectiveness)

Heat maps of Inherent and residual risks (Risk Matrix):

Both the inherent and residual risks shall be measured as Low, Medium, High and Extreme. This can be illustrated in the Heat Map, below:

		1	2	3	4	5
	5	LOW	MEDIUM	HIGH	EXTREME	EXTREME
	4	LOW	MEDIUM	HIGH	HIGH	EXTREME
LIKELIHOOD	**3**	LOW	MEDIUM	MEDIUM	HIGH	HIGH
	2	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
	1	LOW	LOW	LOW	LOW	LOW
Risk Matrix		**1**	**2**	**3**	**4**	**5**
		IMPACT/ CONSEQUENCE				

RISK REPORTING, RISK REGISTER / DATABASE

Risk Registers/ Database

- The Risk Management function shall maintain the registers of all the risks assessed by the various levels of management, in all of the directorates and business units.

- The risk registers should be designed to enable documentation of associated action plans, the risk owners, and action owners who are the officials assigned the responsibility for the implementation of action plans.

- There will be different types of access to the risk registers which will be informed by the profiles of management that must be designed by the Risk Management Unit.

<u>Risk Reporting</u>

Quarterly reports should be generated to enable the processes of risk monitoring and the communication of action plans and the risk profiles as appropriate.

7 ENTERPRISE RISK MANAGEMENT PROCEDURES

7.1 Inherent risk assessments:

Inherent risk assessment is an analysis of the cause of the **uncertainty**, the **likelihood** of this uncertainty occurring, and the **impact** attached to a process or operation, **before** taking into account any existing controls.

The main steps in the Inherent Risk Assessment are: Risk Identification; Risk Analysis; Measuring Risks; and Risk Prioritizing.

Risk Identification

Risk identification involves examining internal and external factors that may affect the achievement of the municipality's objectives. The risk identification process includes Identifying inherent risks associated with each activity and/or business process.

Risks that have been identified will be captured into the Risks Database, and a risk category as per the risk framework will be allocated to each identified risk.

Identification of the Risk Management Universe

The municipality's risk management universe shall be determined by reference to the municipalities:

o Strategic Objectives and Integrated Development Plan, the SDBIP, the national strategic focus areas, government priorities;

o Organizational structure and therefore the various business units;

o Legislative and regulatory requirements;

- o Previous Financial statements, annual reports;

- o Budget information;

- o Organizational Policies and Procedures;

- o External Factors, for example, industry, politics; and

- o Any other relevant information

Business Process Identification and Description, includes

- o Establishing Management objectives and plans for each functionality or business unit in conjunction with Management

- o A description and mapping of the business processes

- o Ascertaining critical activities within each functionality.

- o Identifying the business processes within each critical activity

- o Identifying value drivers

Risk Analysis

The analysis of risks involves analyzing the underlying causes of the risk that may result in the occurrence or non-occurrence thereof, and the analysis of the resultant impact. The main components of the risk analysis stage, in order to identify high risk areas, are:

- Analyzing the likelihood of the risk occurring and the impact thereof; and

- Applying a Risk Rating based on impact and likelihood on a scale of High, Medium and Low.

When analyzing risks emanating from one unit, Management should also consider and analyze the impact thereof on other business units or departments, and related processes. It involves analyzing the impact of the risk on the achievement of both departmental objectives as well as the overall objectives of the organization.

Risk Measurement

This process is largely dependent on the availability of information, and the organization's management information systems. It is critical to measure inherent risk because this information is used to justify the expenditure that will be incurred to either prevent the risk, or realize the benefit from identified opportunity. Risk Measurement can be quantitative or qualitative.

- **Qualitative Risk** analysis is a more subjective approach in which the risk is only assigned a rating of high, medium or low based on the knowledge and judgment of those analyzing and measuring the risk. This approach is appropriate in those instances where there is difficulty in attaching a Rand Value to the identified risk.

- **Quantitative Risk** measurement is a less subjective approach in that the value of the assets at risk is assessed or determined by making reference to available financial information.

- Inherent risk is therefore measured as follows:

(Quantifiable) **Inherent Risk = Potential Loss** (Rand Value) X **Probability of Occurrence**

- **Potential Loss** is the value of the asset at risk, before taking into account any internal control measures or strategies aimed at reducing the risk.

- The assessment of the **potential loss** requires looking at the worst-case scenario; and the outcome of a Potential Loss ranges from catastrophic, to serious to insignificant and these have been defined in the "**Potential Loss Table**".

- Assessing Potential Loss requires the assessment of both tangible and intangible costs that can be attached or assigned to specific assets and processes. The costs may be subject to varying opinions or debate.

- **Probability of Occurrence** is assessed by making reference to the "**Probability Tables**". The Probability levels range from very certain to high to very remote, and each level has been defined in the "**Probability Table**".

7.2   Formal Risk Assessments

The Management of the Saldanha Bay Municipality shall conduct formal Risk Assessments, at least annually, as required in terms of the Municipal Finance Management Act.

The municipality's strategic risk assessments will be conducted at least on an annual basis; or at any time during the financial year when the strategic objectives or strategies are being reviewed.

Annual strategic risk assessments must be integrated with the strategic planning processes of the municipality, at cluster and unit level. The timing of at least the strategic risk assessments should be before or at the commencement of the annual budget process.

Identified inherent risks are categorized according to Extreme, High, Medium and Low. The risk management unit shall design the system to enable the

quantification and categorization of inherent risks, ensuring alignment to good business practices.

The timing of the annual formal risk assessments must fall before or at commencement of the annual budget process. This is intended to enable the financing of the risk management strategies and control systems that should be implemented in order to mitigate identified risks.

The Risk Management function shall collate the results or information collected from the risk assessment process and update the Saldanha Bay Municipality's risk database accordingly.

Custody of the municipality's risks registers and database shall rest with the Municipality's Risk Management function; while update access of the risk registers shall be restricted to authorized individuals.

Strategic and Operational risk assessments will be conducted as follows:

- An enterprise-wide strategic risk assessment process by the Municipal Manager and the Directors shall be conducted at least annually.

- Cluster specific strategic risk assessments by the Directors and Departmental Managers, as well as Supervisors and senior officials as deemed by the Municipal Manager of the Cluster.

- Operational risk assessments shall be conducted at departmental levels by the Managers, senior officials and/or supervisory staff.

7.3   Continuous and Quarterly Risk Assessments

Risk assessments should be conducted for all new activities and/or projects, to ensure that adequate systems are designed to address emerging risks. Unit

management shall ensure that for all major projects, project risk assessments are conducted and action plans in place to address the risk should it materialize.

Management of each department or business unit will be required to continuously assess the risks associated with the activities of their departments. The basis for management decisions must therefore include the results of their assessments of associated risks, and the expected outcomes.

Fraud risk assessments, Information Technology risk assessments, Major Projects Risk analysis should be conducted continuously.

Project risk assessments must be conducted before or at commencement of the project to ensure that events that may impact on project deliverables, project timelines and the budget are identified timorously and action plans are in place to mitigate the occurrence thereof.

The assessment of the residual risk profile requires the analysis of the existence of internal control systems; and if in place whether these are functioning as designed. Alternatively, management should assess whether there are control gaps. The effectiveness of these risk mitigation action plans should be assessed using the municipality's risk assessment tables, as per **Annexure B**.

The implementation of control-self-assessments by management will be phased-in. Upon its implementation, management will be required to submit their control self-assessments the reports to the respective Directors. The Directors will be required to review the control self-assessment and/or the success of the risk management strategies in mitigating the identified risks.

The Executive Management Team should submit the quarterly reports to the Risk Committee, who will communicate due dates of these reports.

The Committee in turn should review and appraise the Executive Management Team accordingly.

7.4   Risk Mitigation Responses /Strategies

Risk owners must ensure that risk mitigation strategies are designed in response to the assessed risks.

The key four (4) risk mitigation strategies are: risk acceptance, risk avoidance, risk transfer and risk control. The municipality recognizes that a combination of the strategies to mitigate risks may be appropriate depending on the nature of the event or activity.

The main objective of a risk mitigation strategy and/or action plan should be to reduce the inherent risk to acceptable residual risk levels, thereby ensuring an acceptable risk profile.

Therefore, the identification, design and implementation of the risk mitigation strategies should be to bring the extreme and high inherent risks down to acceptable levels. Risks and associated mitigation action plans are prioritized according to Priority Levels 1, 2 and 3; with priority level 1 indicating first priority.

The acceptable risk threshold levels are found primarily in the green and yellow shaded areas of the risk matrix or heat maps.

Management shall design and document key risk indicators (KRI's) for all the top risks. These KRI's should be monitored on a regular basis and action plans put in place in case of material changes.

The development of risk mitigation plans should include the responsibility for implementation and associated timeframes.

Priority in the design and development of risk mitigation responses should be guided by the assessed inherent risk levels: i.e. whether extreme, high, medium or low.

Risks to the municipality may be internal or external. In the case of external risks, the municipality does not have control over the occurrence or non-occurrence thereof. However, management is required to design strategies and action plans to mitigate the associated impact to acceptable levels.

The associated decision making levels in the development and implementation of risk mitigation should be in accordance with the delegations of authority; and all steps should be taken to adhere to the municipality's risk management principles.

A key consideration in management's choice of strategy should be the associated cost vs. benefit analysis. The assessment of associated costs vs benefit can be either qualitative or quantitative or both.

It is important that management understands that the mitigation of risks may not necessarily result in the elimination of the identified risks.

7.5   Risk Monitoring

It is critical that the municipality's top risks not within acceptable levels are monitored by management on a monthly/quarterly basis; and by the Municipality's assurance providers on a quarterly basis.

The top risks are those risks that are assessed to be extreme or high and are located in the red and orange areas of the heat maps, respectively.

Accordingly, updated risk reports as designed must be provided to the appropriate authorities, on a monthly and quarterly basis as required.

The Committee and Executive Management Team should monitor the performance of their direct reportees in the implementation of risk management practices and mitigation of key risk areas, at least on a quarterly basis. The monitoring of this KPI must follow the provision and process of the Municipality's Performance Management policy and procedures.

The internal audit function must independently review the action plans as designed and implemented by management to ensure they are effective, efficient and economical; and therefore value adding.

7.6   Risk Communication/ Reporting

Management will therefore be required to submit regular updates of the risk profiles of their business units.

The risk management unit must design reports to meet management expectations, and to enable monitoring of the risk mitigation action plans.

A   Annexure A – Different Categories of risk

Strategic	Strategic Planning / Business Strategy (I.e the SDBIP, the IDP & KPA'S)
	Corporate Planning (Departmental Business Plans)
	Organisational structure
	EXCO Council
	Political Risks [Local government/municipalities]
	Socio-Economic factors
	Industries
	Stakeholder Relations
	Corporate Image
	Political Risks [Provincial and/or National]
	Globalisation risks (effect) – Global Warming, World markets
	Employee Fraud
	Fraud by Service Provider
Financial	Financial Statements / Financial Reporting
	Revenue Management
	Budgets/ budgeting
	Working Capital Management
	Cash Management
	Asset Management
	Debt Management
	Supply Chain Management /Procurement
	Information and Communication Technology
Service Delivery	Electricity
	Water
	Refuse & Waste Removal
	Housing Development & Maintenance services
	Civil Engineering Services
	Electrical Engineering Services
	Public Roads Works & Maintenance
	Local Economic Development
	Property ratings & Valuation roll
	Social Development & Welfare
	Occupational Health and Safety
	Security Services
	Supply Chain Management / Provisioning
	Staff Retention
	Training and Development / Skills Development
	Performance Management
	Remuneration / Employee Benefits
	Employee Relations

	Employee Wellness
	Systems Availability, Integrity and Relevance of Information
	Management Information Systems (Data Warehouse)
	IT Security / Logical Access
	Infrastructure
	Internal Communication
	External Communication (Marketing)
	Media Liaison
	Liaison with Stakeholders
Compliance / Regulatory	Municipal Finance Management Act & Regulations
	Municipal Systems Act
	Municipal Structures Act
	ByLaws
	Labour Laws and regulations
	Black Economic Empowerment / Transformation
	Legal Actions
	Legal Advice
	Contracts Management
	Health and Safety, Environmental
	All other statutory laws and regulations relevant to municipalities

B   **Annexure B – Risk Assessment Tables**

Management will be required to decide on the sizing of the potential risks, the likelihood that it will occur, as well as the adequacy / effectiveness of existing controls. The following three tables are to be used for the respective decisions required during the risk assessment workshops.

1) *Consequence / Impact*

Consequence	1. Insignificant	2. Minor	3. Serious	4. Major/Severe	5. Catastrophic
RMS Outcome description - Qualitative Measures	**Not worth worrying about**	**Consequences can be absorbed, but management effort is still required to minimize its impact**	**Event, which can be managed under normal operating, conditions but require moderate level of resource and management input**	**Significant or Critical event, which with proper management will be endured**	**Disaster with potential to lead to collapse of business and is fundamental to the achievement of objectives**
Service Interruptions	Interruption in a service, which does not impact on the delivery of services or the ability to continue to provide service.	Short-term disruption to service with minimal impact on residents. Locally contained situation.	Some disruption in service with unacceptable impact on residents. Non-permanent loss of ability to	Sustained loss of service, which has serious impact on delivery of residents. Regional	Permanent loss of basic service or facility. Disruption to facility leading to significant 'knock on' effect across

Consequence	1. Insignificant	2. Minor	3. Serious	4. Major/Severe	5. Catastrophic
RMS Outcome description - Qualitative Measures	**Not worth worrying about**	**Consequences can be absorbed, but management effort is still required to minimize its impact**	**Event, which can be managed under normal operating, conditions but require moderate level of resource and management input**	**Significant or Critical event, which with proper management will be endured**	**Disaster with potential to lead to collapse of business and is fundamental to the achievement of objectives**
	Immediate on-site containment.		provide service. On-site containment with outside assistance.	environmental repercussions.	local economy. National service delivery consequences.
Financial Cost/Loss	< R 2 000	< R 10 000	< R 30 000	< R 200 000	> R 200 000
Citizen Feedback	Unlikely to cause complaint.	Complaint possible.	High potential for complaint.	Litigation expected/certain.	Litigation expected/certain.
Adverse Publicity / Reputation	Unlikely to warrant coverage in media and little effect on public	Local media (short term) with minor effect on staff	Local media (long term) with impact on staff morale/public	Provincial media coverage with public confidence of municipality	National media coverage with public confidence of municipality

Consequence	1. Insignificant	2. Minor	3. Serious	4. Major/Severe	5. Catastrophic
RMS Outcome description - Qualitative Measures	Not worth worrying about	Consequences can be absorbed, but management effort is still required to minimize its impact	Event, which can be managed under normal operating, conditions but require moderate level of resource and management input	Significant or Critical event, which with proper management will be endured	Disaster with potential to lead to collapse of business and is fundamental to the achievement of objectives
	confidence/staff morale.	morale/public attitudes.	perception of trust.	undermined.	undermined. Parliament enquiry.
Performance Targets	No impact of targets.	Insignificant impact on municipal targets.	Adverse effect on local and/or provincial and/or national targets.	Failure to meet local and/or provincial and/or national targets.	Failure to meet statutory obligations.
Injury/Harm	No injury or adverse outcome.	Short-term injury of 5 days.	Adverse event which impacts on a number of people. Semi-permanent injury/illness.	Permanent loss time injury having an adverse effect.	Incident leading to unexpected death or major permanent injury to more then one (1) person.

2) Likelihood/Probability of occurrence

Probability Factor	Rating	RMS Occurrence description	Qualification Criteria
Certain	5	Probability of occurrence is certainly once a month	The risk is almost certain to occur in the current circumstances
Likely	4	Probability of occurrence is once a quarter	More than an even chance of occurring
Possible	3	Probability of occurrence is once in 12 months	Could occur quite often
Unlikely	2	Probability of occurrence is once in five years	Small likelihood but could happen
Rare	1	Probability of occurrence is once in twenty (20) years	Not expected to happen - Event would be a surprise

3) Control Effectiveness/Adequacy

Effectiveness Factor	Rating	RMS Control description	Qualification Criteria
Very Good	90%	Could not be more effectively implemented to mitigate the risk	Risk exposure is effectively controlled and managed
Good	80%	Most risks are effectively controlled and mitigated	Majority of risk exposure is effectively controlled and managed
Satisfactory	65%	There is room for improvement in the control system	There is room for some improvement

Effectiveness Factor	Rating	RMS Control description	Qualification Criteria
Weak	40%	Some risks appear to be controlled but there are major deficiencies	Some of the risk exposure appears to be controlled, but there are major deficiencies
Unsatisfactory	20%	The control system is ineffective	Control measures are ineffective

The Committee shall review the Strategy annually or when changes in legislation so required and recommend to the Council for approval any amendments that may be required.